CHALMERS

Architectures and standards for hardening of an integrated security system

Master of Science Thesis in the Programme Networks and Distributed Systems

PETTER NORDLANDER

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, August 2010

Standards and Architectures for Hardening of an Integrated Security System

PETTER NORDLANDER

Examiner: ROGER JOHANSSON

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden August 2010

Architectures and Standards for Hardening of an Integrated Security System

PETTER NORDLANDER
Department of Computer Science and Engineering
Chalmers University of Technology

ABSTRACT

Physical security systems, such as bulgar alarms, surveillance cameras and door access control systems are becoming more and more advanced. To be able to use the increased functionality and to reduce the needed infrastructure, they are also typically connected using TCP/IP and integrated in a centralized security system. This integration allows for remote administration and intelligent software solutions. However, this progress opens up such integrated security systems for cyber attacks.

This study gathers the cyber threats and risks that applies to integrated security systems. Then a few major cyber security guidelines and standards on the market are analyzed to get a set of security practices that are applicable to integrated security systems. Based on the security practices learned, a hardening architecture is proposed for an integrated security system featuring surveillance cameras, bulgar alarms and access control with remote access.

The results show that there are many threats directed towards integrated security systems. The guidelines studied gives a good foundation for cyber security but the practices has to be somewhat tweaked to fit integrated security systems. By using smart firewall design with encrypted VPN to segment the network tightly, most threats can be eliminated without much complexity overhead.

Keywords: Integrated security systems, physical security, digital control system, security

PREFACE

This report was produced as the result of a master thesis project at the department of Computer Science and Engineering at Chalmers University of Technology. The work was commissioned by Peelit AB and conducted at their office in Partille from January to May 2010.

The project comprises 30 university points and is the mandatory final step towards a Master of Science degree in Computer Science and Engineering.

ACKNOWLEDGEMENT

This thesis would not have been possible without great assistance, inspiration and knowledge from Fredrik Pihl, CEO at Peelit AB. I am also thankful for the invaluable support from my entire family.

CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

As the need for physical security increases and the technology in embedded systems becomes cheaper and more advanced, there is an increasing trend in integration of security systems. As an outcome, the usage of ethernet and TCP/IP as well as common desktop operating systems, usually found in the office/administrative IT world, is now widely used as an integrated part of modern integrated security systems. The problem is that, while integrating physical security infrastructure with office IT infrastructure, threats and security issues from both worlds meets. Now might be the time to start thinking cyber security in the physical security world. One major issue when doing this is that there is no real documentation and governmental guidelines for cyber security in integrated security systems. There are, however, a lot of guidelines regarding cyber security in industrial control systems, of which integrated security system can be seen as a sub set. This project is done in collaboration with Peelit AB. It is a company that provides integration software for physical security systems as well as IT security solutions.

1.2 PURPOSE

The core purpose of this project is to provide an hardening architecture for integrated physical security systems from a cyber security perspective. The architecture should attempt to provide sufficient security for usage in facilities with a high security profile. A set of standards and guidelines for cyber security in information system and digital control systems should be used as a foundation for the architecture. An analysis of the standards should be provided with respect to the various threats and risks that concern an integrated security system.

1.3 GOAL

- Identify the threats and risks with a generic integrated security system with respect to cyber security.
- Analyze applicable security standards and guidelines on the market to find out how well they match the need of integrated security systems.
- Construct a generic hardening architecture to increase the cyber security of integrated security systems. The architecture should comply with the analyzed standards as close as possible.

1.4 SCOPE

Since the possible setups of integrated security systems are infinite, it is very hard to provide a general architecture without being too general. Therefore, only one of the most common installations will be covered. Also, only architectural and technical details will be handled. Administration, procedures, usage patterns, auditing and other parts of security is not in the scope of this thesis. The reference system setup is based on the following components

- One Security system server with integration functions
- One or more supervision clients, used to monitor the security system
- One or more intrusion detection system(s)
- One access control system, including a server
- One CCTV (Closed-circuit Television). That is one VMS (Video Management Server) system and one or more cameras.

As a security component for remote access, a VPN gateway is also to be configured. The system setup assumes an Internet connection but does not assume the presence of an office/administrative TCP/IP network in the same building. An administrative network should not complicate or interfere with the security system though.

The architecture is to be based using a selection of guidelines and standards. Swedish Emergency Management Agency has guidelines for both information systems and digital control systems. Both are included in this study.

- Swedish Emergency Management Agency: Basic level of information security (BITS).
- Swedish Emergency Management Agency: Guide to Increased Security in Process Control System for Critical Societal Functions
- U.S. Department of Homeland Security: Control System Recommended Practices.
- U.S. National Institute of Science and Technology: Guide to ICS cyber security

The main question to answer regarding this reference system is – how to harden an integrated security system. While this thesis is done in collaboration with Peelit and the purpose of this project is to make installations of the product AppVision.NET more secure, this thesis does not assume the use of AppVision.NET, or any other specific product, unless explicitly stated. The idea is to take a more general approach that does not rely on a specific product or version.

2 THEORY

This chapter describes the theory of the key components that used to secure a network. This includes firewall technology for securing networks, encrypted communication and the structure of physical security devices.

2.1 FIREWALL BASED NETWORK SECURITY

A firewall is a generic term for a device that enforces security policies on a network that is connected to other networks. There are several types of firewalls as well as there are several ways they are implemented. This section discusses the most common types of firewalls and how they are typically used.

2.1.1 PACKET FILTERING FIREWALLS

Packet filtering firewalls are the most basic form of firewalls. They implement very simple sets of rules, often known as Access Control Lists, ACL. The rules are limited to stateless information. That is, no information about previous events, and only information found in the network- or transport layer protocol. The core protocol in this case will be any protocol in the TCP/IP stack, such as IP, TCP, UDP and ICMP. The most basic form of packet filter rules is defined by the parameters of address, port, protocol (TCP/UDP/ICMP) and interface. Table 1 shows an example of rules to implement a strict firewall only letting traffic from the 10.0.0.0 network to port 80/TCP, which most likely is HTTP, pass [Fielding, 1999].

Interface	**Source network**	**Destination network**	**Source port**	**Destination port**	**protocol**	**allow/deny**
Eth0/1	10.0.0.0/24	Any	Any	80	TCP	Allow
Eth0/1	Any	Any	Any	Any	Any	Deny

Table 1: Example of simple Packet filtering rules, only passing port 80/TCP in one direction

Another feature that can be done with packet filtering firewalls is to remove malformed packets, that can cause denial of service. There will be more about malformed packets later in this chapter. Even though there is a lot of security issues that cannot be addressed with such a limited set of rules and logic, there is an advantage that a packet filtering firewall can be implemented in almost any device. There is built in support in all major operating systems by default. Packet filtering is usually implemented in border routers, which will provide a very fast first screening firewall function [Henmi, 2006].

2.1.2 STATEFUL PACKET INSPECTION

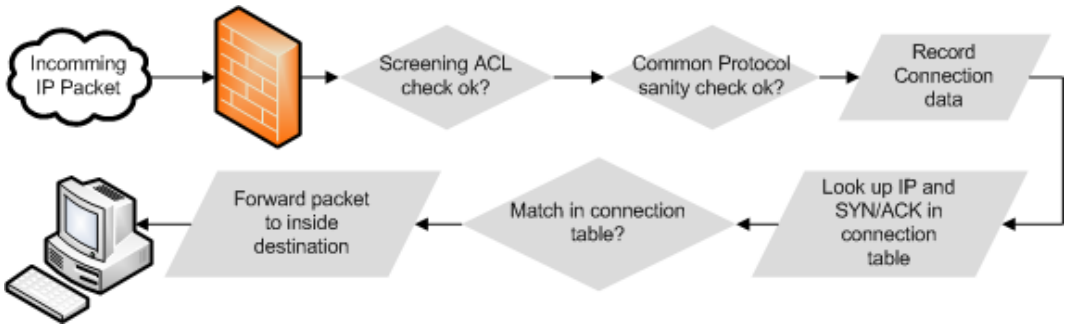

Illustration 1: Stateful Packet Inspection flow from external network to internal host

To enhance security, but without adding much more complexity of a system, the states of packets can be added to the firewall inspection. Stateful packet inspection works by recording connection states between different hosts. Only incoming packets that are in an existing connection and applies to packet filtering rules (ACL) might be allowed. Also some basic sanity check of malformed protocols might take place here. Note that only common protocols such as SNMP or HTTP are checked to avoid obvious rubbish packets. The process of inspection in illustration 1 is for TCP connections. TCP packets are connection based, using SYN, ACK and FIN flags to setup, maintain and close connections. This makes it very easy to track connections using TCP. UDP and ICMP connections, that really are no connections, but rather a stateless exchange of packets, can be tracked in similar fashion, but instead of using SYN/ACK flags, timing and other information will be used. Because of that, non TCP connections are less reliable to track. [Henmi, 2006].

2.1.3 OTHER FIREWALLS

Proxy type firewalls is another firewall type that is used in special circumstances. It works on supported protocols only. That is, the proxy has to be designed for one kind of application protocol. It is common to use proxy firewalls with HTTP traffic for instance. The proxy firewall actually terminates the connection from the client to the web server. Then it examines the HTTP packet, if it can pass a set of rules, the proxy then establishes a connection to the web server, sending through the HTTP packet and getting the response packet, which is passed to the client. There is usually two different usages of proxy servers [Panko, 2010].

- Protecting client computers from potentially malicious web servers
- Protecting sensitive web servers from potentially malicious users.

2.2 ENCRYPTED COMMUNICATION CHANNELS

2.2.1 ENCRYPTION ALGORITHMS

This text is not intended to be a complete theory about encryption. However, a few common algorithms and usage areas will be pointed out.

Hash functions are functions used to provide integrity of a message. There are three basic properties of a hash function

1. The calculation of a message digest, h(m), should be very quick
2. The hash function h should be one way. That is, it should be very hard to find *m*, given *x* where *x = h(m)*.
3. It should be hard to find messages *m1* and *m2* where *h(m1) = h(m2)*

In practice this results in a function taking a message of arbitrary length and produces a fixed size message digest. For most hash algorithms, that means mapping a message of arbitrary length to a 128-512 bit message digest. Common in use today is the MD5, Message Digest 5, algorithm and the Secure Hash Algorithm, SHA-1 and SHA-2. MD5 is considered weak, producing a 128 bit message digest. The SHA-1 algorithm produces a 160-bit message digest. A more secure version of SHA, SHA-2 has been developed by NSA. It supports 256 and 512 bit hashing [Trappe, 2006].

To transmit a lot of data with high performance, a fast encryption algorithm has to be used. There are two common standard algorithms used today, DES and AES. Both use symmetric key encryption. That is, the same key can be used to encrypt and decrypt the data.

DES, Data Encryption Standard, has long been the standard algorithm for bulk data encryption. It was designed by IBM and modified by NSA. DES is a block cipher with 56 bit key size. It has now become outdated and can be broken with brute force attacks. Since the algorithm has been implemented on a lot of systems, it is still in use, but used three times. This variation is called 3DES and uses three keys. The algorithm works like this: $c = E_{K1}(D_{K2}(E_{K3}(m)))$ where E = DES encryption and D = DES decryption. Running DES three times gives a key strength of approximately 112 bit. The 3DES, even though it is rather secure, will be slow when performing encryption three times [Trappe, 2006].

AES, Advanced Encryption Standard is a more recent standard for encryption. It uses an encryption algorithm called Rijndael. It handles key sizes of 128, 192 and 256 bit. AES was set as the encryption standard by NIST, National Institute of Science and Technology. Without going into the detail it is a lot faster and more secure than 3DES. A brute force attack that would break DES in one second would take 100 trillion years against 128 bit AES [Panko, 2010].

2.2.2 SSH

Two important protocols used across the Internet is telnet and FTP. Telnet is used for remote shell access and FTP is used for file transfer between hosts. Neither of these protocols has any security. The SSH, Secure Shell, protocol was developed to replace them both in sensitive environments. This section refers to the SSH-2 protocol, which is the most common today [Panko, 2010].

The main reason SSH is included here is not to be used for remote shell access or file transfers. The one feature of interest in SSH is port forwarding. SSH port forwarding is used to create a TCP tunnel from one ip/port, encrypt it, decrypt it at the SSH server and then pass it on to the destination ip/port.

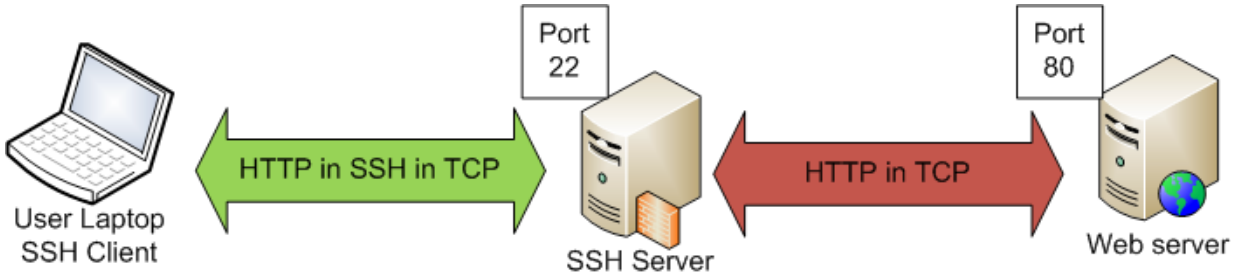

Illustration 2: SSH port forwarding. The SSH server connects to a specific host/port and forwards the connection to the client encrypted

SSH authentication and encryption is done by cipher protocol suite that is negotiated upon at the beginning of the session. It will be standard protocols like RSA, DSA, Kerberos, Diffie-hellman, AES, SHA-1, etc. However, they are used for different things. The main problem during authentication is to avoid MITM attacks. That is, the client must not connect to any other SSH server than the intended server. The authentication protocol works like this:

1. A session ID, H, is constructed. It is constructed in such a way that neither side can enforce its value. It is also unique for each session. Along with session ID, H, a shared secret, K, is negotiated to be used in further cipher protocols.

2. The first time the client connects to the server, it receives the public host key for the server. That is, it is important that this initial connection is done in a controlled environment. The host key for this server is stored locally on the client.

3. For future connections, the server signs the session ID using its private host key, then the client can verify that the the integrity of the communication. The session ID cannot be forged, so that makes sure a MITM attack is not possible.

4. An encrypted connection is set up, using the selected encryption algorithm (such as 3DES or AES128).

5. The client verifies itself. This can be done using using public key authentication, but usually a simple user/password is supplied and verified by the server, who then decides whether to drop or keep the connection [Barret, et.al. 2005].

2.2.3 SSL

Secure Sockets Layer (SSL), was developed by Netscape to secure the HTTP protocol in the mid-1990s. SSL in this report, however, will refer to both SSL and its close spin off, Transport Layer Security (TLS), which has some minor differences.

When a client connects to a server using SSL, a cipher suite is negotiated. This contains ciphers for public key (RSA, Diffie-Hellman, etc.), block cipher encryption (3DES, AES, etc.), hashing (SHA-1, MD5, etc.) and data compression (PKZip, etc.). The authentication is then performed:

1. Client → server: Cipher suite (we assume RSA is used), version number, 4 byte time stamp + 32 random bytes, $\{R_c\}$.

2. Server → client: 4 byte time stamp + 28 random bytes, $\{R_s\}$, selected cipher suite, X.509 certificate.

3. Client → server: 48 bytes “pre master key” $\{S_{pm}\}$, encrypted with the servers public key from X.509.

4. The master key is then computed on each side, + means concatenation here. A, B, C is padding. The master key is secure from replay attacks by eavesdroppers since the time stamps are embedded.
   MD5(S_{pm} || SHA-1(A || S_{pm} || R_c || R_s)) +
   MD5(S_{pm} || SHA-1(BB || S_{pm} || R_c || R_s)) +
   MD5(S_{pm} || SHA-1(CCC || S_{pm} || R_c || R_s))

5. The master key is then used to produce keys for block encryption using the same method used to construct the master key. Six keys are constructed. Three for each direction. One is for block cipher encryption, one is used to sign messages (the authentication key), and one is used as an initialization value for the block cipher.

6. The communication can then continue encrypted using the selected block cipher (AES for instance), and the calculated key. Each message is signed using: HASH_FUNCTION(MessageData + AuthenticationKey). This hash is then included in the encrypted message to ensure integrity.

Clients can also supply certificates to verify its identity, but it is seldom done. Most SSL applications rely on some application specific user authentication instead. Such authentication can be credit card numbers, user password etc. [Trappe, 2006].

2.2.4 IPSEC

IPSec, Internet Protocol Security, is a family of IETF cryptographic standards. IPSec provides security on the network layer by providing confidentiality and integrity to ip packets. It was first introduced to IPv6, but has been extended to work on IPv4 as well. The idea is to provide transparent security for the transport layer and above. There are two distinct forms of IPSec. One is called tunnel-mode and handles site-to-site encryption and is shown in illustration 3. Tunnel mode is easier to set up and manage and is possible to use in combination with firewalls and NAT. The other form is called transport mode. It encrypts traffic from source to destination and does not require specific gateways. It requires certificates on each device. Transport mode is often incompatible with firewalls, since firewalls cannot decrypt the content of the packet and decide whether to filter the packet or not. Transport mode is shown in illustration 4.

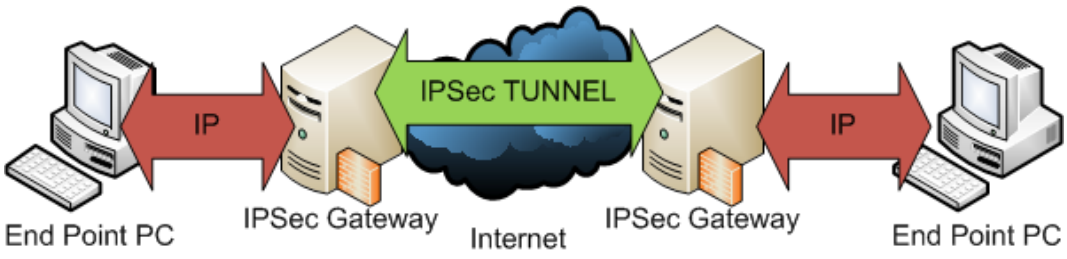

Illustration 3: IPSec, tunnel-mode, provides security between two gateways but not within the local networks.

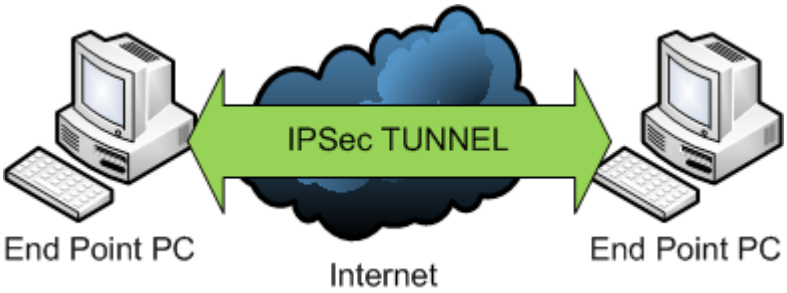

Illustration 4: IPSec, transport-mode, provides end-to-end security.

A established IPSec connection is called a Security Association, SA. The authentication procedure uses the IKE, Internet Key Exchange, standard protocol. The procedure is done in two steps.

Step 1 – Establishing IKE protection

1. The cipher suite is negotiated.
    1. Encryption algorithm (3DES, DES, etc.)
    2. Integrity algorithm (SHA-1, MD5, etc.)
    3. Diffie-Hellman settings
    4. Authentication method (pre-shared key, certificate, kerberos)
2. The key is exchanged using Diffie-Hellman. A master key is generated at each side.
3. The master key is then used to secure the rest of the authentication process. The master key is used together with the selected cipher suite. The key exchange is authenticated to prevent MITM attacks. IPSec uses a set of identity types for the authentication process (IPv4 address, qualified domain name, pre-shared key, certificate properties etc.), which type depends on the authentication method chosen.

Step 2 – Security Association for data communication between two computers

1. Policy Negotiation
    1. Cipher suite is negotiated
        1. IPSec protocol. Essentially: Consider confidentiality and integrity, or only integrity

2. Integrity algorithm (SHA-1, MD5, etc.)
3. Encryption algorithm (3DES, DES).

2. Then the SA is done. One SA for each direction is established.

2. Session key information is exchanged and refreshed if needed
3. The SA and key information is used to establish a secure IP connection.

[Panko, 2010]

2.2.5 VPN

VPN, Virtual Private Networks, is a way to use an insecure communication network to transmit arbitrary traffic, and thus be able to access features inside for instance a company's internal network from hotel rooms, mobile broadband and home connections. It is also a way to save money for companies when they do not have to buy dedicated communication channels between branch offices, headquarters and partners. Instead, they can simply buy a shared Internet connection and utilize VPN. There are several deployment models for VPN. Some are hardware based, some features encryption and there is several technological solutions for it. The core idea behind VPN is that remote locations should be interconnected as one logical network. As such, the same internal security policies can be implemented across all sites, without worrying about malicious users at Internet being able to break into the VPN connection.

One common solution is a totally transparent layer-2 based solution. This can be done by using various technologies, such as MPLS – Multi Protocol Label Switching. This solution is efficient, does not reduce performance, is scalable and provides features such as bandwidth reservation. It does not supply enhanced security such as encryption. It requires the ISP to offer that service, which also requires the ISP to have a dedicated connection from site A to site B.

To implement a VPN across Internet, there are many solutions. Almost all solutions are vendor specific. Technologies like IPSec, SSL and SSH can be used to tunnel data between two VPN end points [Henmi, A. 2006].

Any advantage or disadvantage of the technologies can partially be overcome by vendor specific drivers. For instance, it is possible to tunnel arbitrary TCP/IP traffic using SSL VPN by some vender solutions. This effectively makes protocols like SSH and SSL work in the transport layer or even the network layer in some specific cases [Panko, 2010].

2.3 INTEGRATED PHYSICAL SECURITY SYSTEMS

Before starting to analyze the threats and risks that are specific to integrated security systems, then one must understand the very nature in which they exists. Physical security systems, especially modern, ip-based, integrated security systems, reside in many domains. It is a special kind of an industrial control system but there are a lot of differences in architecture and usage between these two system kinds. The physical security systems has recently started to become IP based systems [Fleisch, 2003].

2.3.1 CCTV

Video Surveillance, or CCTV – Closed Circuit Television – systems are a network of cameras to display live video or record video on recording servers. Cameras are often IP based and require a lot of bandwidth to stream high resolution video. There are also analog cameras that uses analog to digital converters to encode the video to the recording servers. The servers often require high performance hardware to perform video analysis. [Norman, 2007].

2.3.2 ACCESS CONTROL SYSTEMS

Access control systems are used to control physical locks on doors and other physical gateways. The locks are controlled by a central or local control system that integrates with the security integration server. To authenticate users, key pads and card readers, often both combined, are used. The card readers can be TCP/IP based or user some proprietary communication hardware [Norman, 2007].

2.3.3 BULGAR ALARM

Bulgar alarms uses a central controller system and many connected sensors. Each sensor is typically connected using simple electric wires. The sensors will react on different kind of intrusions, such as motion detectors, open door detectors and broken glass detectors. The system also typically features control panels, such as key pads to operate the system. All integration are with the central controller [Norman, 2007].

2.3.4 NETWORK AREA COVERAGE

An integrated security system will be present in pretty much all places in the facility which it has been installed. All important doors, including outdoor gates, will have access control panels and devices, all windows and rooms will have intrusion detection sensors and all important rooms as well as the outdoor perimeter will have surveillance cameras. The software will be located on servers placed in a server room and monitoring client

stations will be placed in reception desks, office rooms and security monitoring centrals [Norman, 2007]. This setup requires a huge TCP/IP network that covers a large area. It has been seen in the business that there are demands to reuse the existing administrative IP networks to save money [Fleisch, 2003].

2.3.5 PHYSICAL PERIMETER PROTECTION

One common best practice when protecting sensitive computer and control systems from cyber threats is to physically lock them in and only admit authorized personnel entrance to the systems.[SEMA,2006], [Stouffer, et.al, 2008]. However, this is obviously not possible with physical security systems, since they, by nature, reside on the outside of the perimeter guarding the inside. The terminals and equipment will be exposed to threats from the outside, and normally is hardened to withstand and deal with physical threats. What about cyber threats then? To what point does it matter that the RJ45 Ethernet connectors now are located outside the builds, connecting CCTV cameras?

This discussion raises questions that might be out of the scope to dig deeper into within this study, but is worth mentioning, none the less. As previously mentioned, restricting physical access to sensitive computer based systems is one important cyber threat mitigation strategy used. How is the risk calculation affected by the cyber security level in the physical security system used to protect the sensitive computer system? I will not go any further on this subject but provide a strategy to harden an integrated security system to, hopefully, reduce the need to ask such questions.

2.3.6 USAGE PATTERNS

There is two drastically different user groups of integrated security systems. First of all, there is the everyday users of the security systems by themselves. That is, people accessing the physical building and holders of access codes and access mediums, such as entrance cards, RFID tokens etc. These users will almost never interfere with the integrated system. In fact the features of the system that such user can do are mostly to lock/unlock perimeter gates such as doors and turn on/off the intrusion detection system. Of course, there are a few variations, such as delayed, timed door access, turn on different intrusion detection zones and the use of different authentication tokens, such as biometric, smart cards, pin codes etc. [Smart Card Alliance, 2005]. However, there will be no more focus on this user

groups in this report, since it will not interfere with the system integration. The other group of users that will be discussed is the administrators and operators of the integrated system. Besides installation technicians and it support personnel that might need access to the system to set up or configure it correctly, there are the every day operators. These might be security personnel monitoring the security of a facility, Security officers and likewise. [Norman, 2007]. These operators will have a varying degree of access to the total physical security system of the facility. From read only access to full, unrestricted access, including access to change log files, change the behavior of each connected device etc. The users (or operators) have to access the integrated system from various places – office, remote office, home office, the reception and in a dedicated control room. In reality – anywhere where there is an Internet connection. Today with mobile broadband access – that is actually everywhere.

3 METHOD

3.1 APPROACH

The process of this study is divided into three parts. The first part will analyze the security risks and threats to an integrated security system. When that is done, in part two, an analysis of the chosen guidelines and standards will take place. The analysis is made to gather the baseline of techniques that can be used to protect an integrated security system. Since the guidelines are not directly written to match physical security systems, the analysis has to select which parts of the guidelines are usable and which are not. Part three of this study is to form a cyber-security best practice when installing integrated security systems. The goal is that the outcome system will be hardened to withstand computer based attacks.

3.2 BACKGROUND AND QUESTION TO ANSWER

The primary factor in the nature of physical security systems that needs to be examined is the fact that the security of the security system itself might be a problem for that security of other systems in the same facility. Consider this fictive example.

An important organization (A) has very valuable information stored inside servers in the headquarter building. A counter organization (B) wants that information by any means and has resources at disposal. Of course, organization A have installed a top of the line,

integrated, security system to physically protect the important servers. Besides that, a high end IT security system has been deployed to protect the servers from cyber threats. What are the options to acquire this information, for organization B, given that the employees of organization A are loyal and cannot be bribed?

It is as hard to break into the building by force as it is to hack into the computer system and steal the information. These both access ways have been foreseen and preventive actions and security systems has been installed to counter such attempts. The question is, is it possible to hack into the physical security system, fool it, and then physically break in and steal the information?

3.3 REFERENCE SYSTEM SETUP

To be able to identify security risks and provide guidelines to harden an integrated security system, a precise reference system has to be defined. Given the reference system defined in the scope section of the introduction chapter, some more assumptions has to be made.

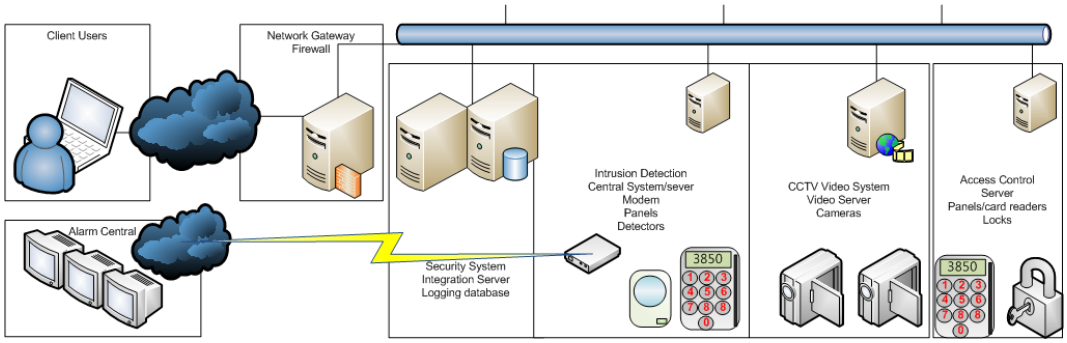

Illustration 5: Reference system. Integration of CCTV, access control and intrusion detection

As can be seen in illustration 5, three security systems are connected to an integration server. Connections to the integration server and the security system in general are made through some kind of gateway or firewall. This chapter gives some detailed assumptions about each part of this system.

3.3.1 CLIENT WORKSTATIONS

Client workstations are assumed to use some common, well known operating system (such as Microsoft Windows and Unix including Linux and Mac OS X) and common PC hardware. The network connection to the client is assumed to be hostile. Weather the network are a public wireless hot-spot, mobile broadband, home Internet connection, dial-up, regular office network or a dedicated security network connection does not matter

since the system is supposed to support remote access. All connections will be treated equally hostile, according to the worst case scenario. The client software is assumed not to be run in a web browser, but as a standalone program.

3.3.2 INTEGRATION SERVER

The integration server is the primary target for this study. To reduce the complexity of the architecture, the integration server is assumed to be one single physical unit. In reality the system might be represented by several physical hosts for redundancy/ load balancing purposes. The integration server also features a database server for storage. All integration between the different sub systems will take place in this server, such as logic that synchronizes and makes for instance the access control system interact with the CCTV system.

The integration server is also the access point for data and access to data in the system. The remote security clients will connect to this server to receive graphical presentation of the security system status and to control and administer the system.

3.3.3 NETWORK GATEWAY

There should be some kind of network gateway connected to the system, to connect it with remote clients. The specific configuration and operational details is left unspecified at this point and will be part of the hardening solution of this study.

3.3.4 CCTV SUB SYSTEM

One CCTV system is connected. The cameras send their video to one or many video recording servers. In this case, we refer to only one for the sake of simplicity. In reality many recording servers are needed for a large installation to provide enough computational power. The cameras should communicate with the recording server through TCP/IP, although analog cameras can be used in combination with analog-to-digital video encoders.

3.3.5 ACCESS CONTROL SYSTEM

One access control system should be connected. That includes locks for doors, key pads with card readers and a central controller. The card readers are connected with proprietary data communication wires or with standard TCP/IP. The controller might also contain a software or hardware module with pc-client access to administer the users and rights.

3.3.6 BULGAR ALARM SYSTEM

A bulgar alarm system – intrusion detection system – should be connected. This includes sensors, key pads and a central controller. The integration and TCP/IP communication is connected only to the central controller. An external connection, such as modem or ISDN might be connected to this controller as well.

3.4 ANALYSIS OF THREATS

An analysis of threats and potential vulnerabilities that might affect an integrated security system will be performed. The analysis will be performed at each tier in the security design, that is: threats against the system perimeter, attacks from the internal network and attacks against towards the applications and their hosts. Each single, specific, detailed threat will not be covered, but instead the focus is to include all major different forms of it-security threats against an integrated security system from a top down view.

3.5 ANALYSIS OF STANDARDS

This analysis of the standards and guidelines that this study is based upon is conducted to verify to what extent they can mitigate the threats to this particular kind of integrated security system. It is also an analysis to verify the compatibility with an integrated security system – if all measures the standard proposes are possible to perform.

3.6 HARDEND ARCHITECTURE

This step is the final step, and will try to provide a hardened architecture to provide as good IT security as possible without adding too much complexity to the system. Specifically, the architecture comply as close as possible with the standards that are studied. The architecture should not re design or restructure the sub systems (CCTV, access control and bulgar alarm).

4 ANALYSIS OF THREATS AND RISKS

An integrated security system can be attacked with a lot of different approaches. The complexity increases as more users connect to the system. There is the alarm central, office computers, VPN to remote offices computers, edge devices, modem connections and internal threats [Norman, 2007]. Some common connections to an integrated security system is shown in illustration 6 and there are some ideas where an attacker might be located.

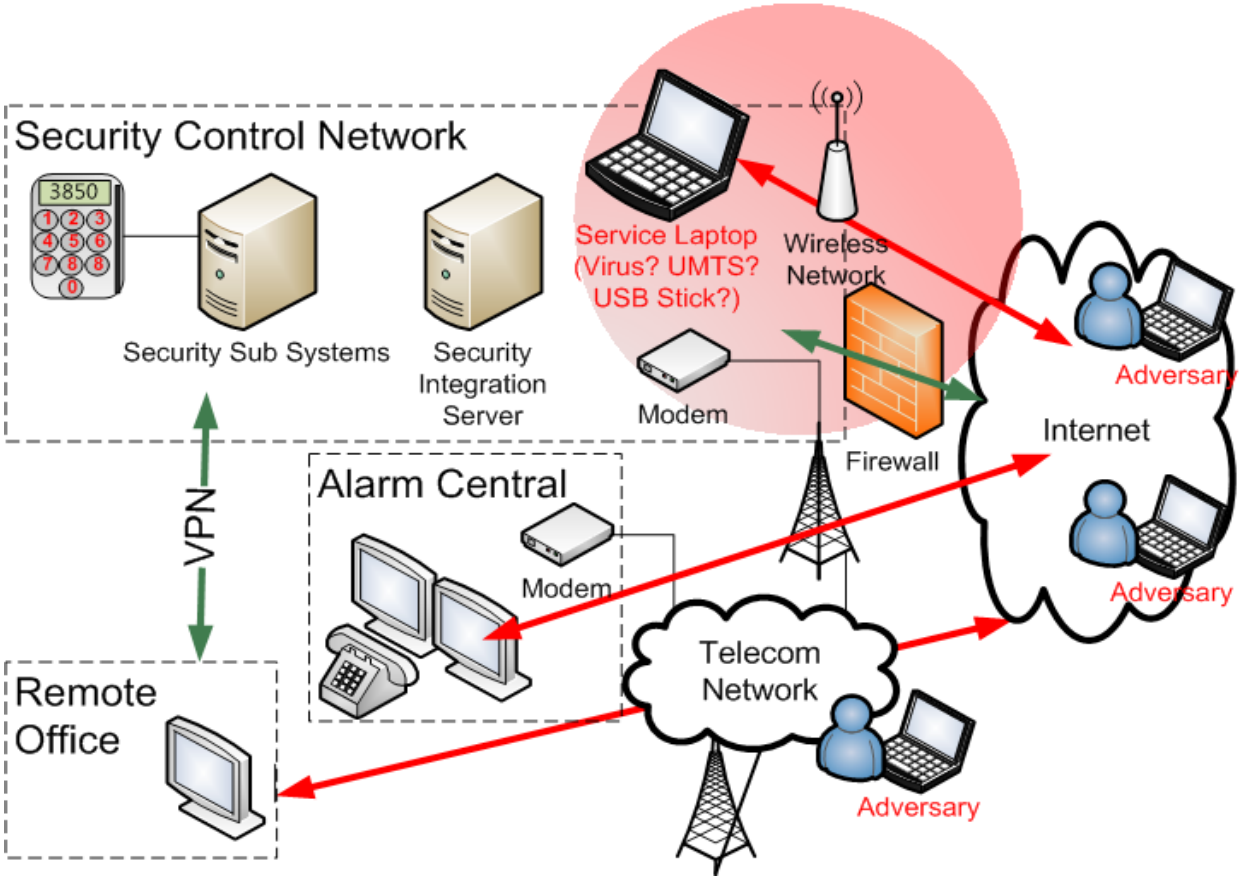

Illustration 6: The threat complexity for an integrated security system. Green arrows shows secure connections. Red arrows shows potential entry paths for adversaries.

4.1 SYSTEM SENSITIVITY

The required sensitivity of a computer system can be described in terms of confidentiality, integrity and availability. Confidentiality reflects the ability to keep information secret from unauthorized users. Integrity is the ability to prevent unauthorized users from modifying information. Availability reflects the ability to keep a sensitive system operational at all time. Specifically, the ability to keep unauthorized users from interrupting or disturbing the service provided by the system. There are some differences between regular corporate IT systems and integrated security systems. A typical corporate IT system will require high confidentiality and integrity to protect important information. However, high availability is not equally important, since users probably can wait a few moment to retrieve a document or to check the mail without to much damage done [Homeland Security, 2009]. For security systems, availability is of great importance. The main target for attackers is to disable the security system. Only a small time of system down time can be enough for a robbery or a threat to the security of important subjects. This is a general view, the requirements of security aspects might vary dependent each specific situation. Integrity is also important for security systems.

Security monitor personnel and guards relies heavily on the fact that the camera images they see has not been modified, the status of burglar alarm is correct etc. However, even though not totally unimportant, confidentiality is of less concern to security systems. In many cases alarms are all but confidential, for instance loud sound and light signals on unauthorized intrusions [Norman, 2007]. The attacks against an integrated security system can categorized into methods of breaking the confidentiality, integrity and availability respectively.

	Confidentiality	Integrity	Availability
Typical IT systems	High priority	High priority	Low priority
Security Systems	Low priority	High priority	High priority

Table 2: The difference in priority of security aspects in typical corporate IT systems and security systems

4.2 TYPES OF THREATS AND VULNERABILITIES

The threats and vulnerabilities taken into account will be presented in three tiers. This represents a common flow of an attack [Panko, 2010]. Tier one is vulnerabilities of the system perimeter. This will usually be the first step an attacker attempts. Tier two is threats against the system given that an intruder has network access to the system. In this step, the attacker usually gathers various information from the network. This information can be valuable in it self, but is usually needed in tier three where the attacker exploits vulnerabilities to take control over devices and applications.

4.3 TIER ONE - SYSTEM PERIMETER

For an attacker to be able to perform any IT-based attack against the security system, as a first step, some kind of communication with the system has to be established. As can be seen by the arrows in illustration 6 there are many possible ways past the network perimeter of a common integrated security system. Taken into account the principle of easiest penetration [Pfleeger, Pfleeger, 2007], the attacker will take the least cumbersome entry path. Therefore, the security of the perimeter is only as high as the least secure way in.

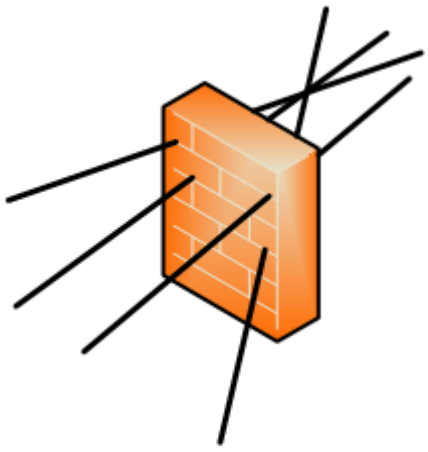

Illustration 7: A firewall with many applications passing though is less secure

4.3.1 MAIN FIREWALL

The first thing to think about is the main firewall that filters traffic to and from the Internet. A common vulnerability is that the firewall handles a lot of applications inside the network and

therefore has to let a lot different traffic past [Olovsson, 2006]. In integrated security systems, this can be services like system administration, database connections, integrations to other systems, CCTV media streams, access control administration, alarm passing etc. The firewall look like a Swiss cheese at worst, as seen in illustration 7.

4.3.2 REMOTE ACCESS/VPN

The point with VPN solutions that provides remote access for mobile clients is that the client should have a way past the main firewall to access internal network resources [Henmi, 2006]. The vulnerability is not usually the VPN encryption itself but rather the client. An insecure mobile client (laptop, smart phone, etc.) that connects to an integrated security system over the Internet, can easily be taken over and used to access the internal corporate security system. The same analogy applies to client connections from less secure networks. This, by some means, also applies to dual homed hosts where one client is connected to two networks with different security policies. Shinder writes about split tunneling and some preventive measures on a Microsoft Windows environment [Shinder, 2005]. However, it shows that in the worst case, a single weak configured client can provide a high speed route into the security system that bypasses the firewall. Illustration 8 gives an idea about the connection.

Illustration 8: Split tunneling allows captured or misconfigured VPN clients to be an open gate into the network

4.3.3 BACKDOORS

Except for the main Internet firewall and VPN connections, there might be other backdoor gateways to access an integrated security system network. One way is through modems and dial-up lines that are connected to remote alarm centrals. Another potential backdoor to enter the system is through insecure wireless networks that might be connected to the security system network [Norman, 2007]. The backdoors listed above might have some protection and some special requirements to exploit, such as being in the range of the wireless network. It is none the less important to be aware of the potential threat.

4.4 TIER TWO - INSIDE NETWORK THREATS

Once the attacker has some kind of access to the internal network of the integrated security system, there are a series of threats that might be dangerous for the system. This kind of attacks can be performed by someone who has succeeded in an attack in tier one, or by a virus that has made its way into the system. This might also applies to “insiders” or evil employees that have access to the network equipment but are unauthorized to use the security system. Succeeding attacks at this tier might interrupt system operations or provide the user with sensitive information.

4.4.1 DENIAL OF SERVICE

As previously stated, a key requirement for an integrated security system is availability. A consequence of the purpose of a security system is that an antagonist (thief, intruder, etc) will be happy to disable the security system for a while. There is a variety of techniques to perform denial-of-service (DoS) attacks. There are ways to exhausting network resources, to make valid network traffic unable to get through, such as flooding. Another vulnerability found in the past on computers is malformed network packets. Some operating systems could easily crash if they receive malformed packets [Pfleeger, Pfleeger, 2007]. This problem with handling malformed traffic has been fixed in most modern operating systems. However, today, as more and more of the edge devices is directly connected to the network; these vulnerabilities might still be present. This has been seen in mobile smart phones connected to networks [Habib, Cyril, Olovsson, 2009]. Although there is no present, public study on the network protocol stability of physical security edge devices, this at least poses a threat to devices not verified.

4.4.2 EAVESDROPPING

Eavesdropping is straight forward. It can be as simple as an unauthorized user listening to plain text traffic on the network. Since confidentiality is not a major concern for integrated security systems, this might not be a great threat. However, eavesdropping can have some bad side effects, considering defense-in-depth strategies. It is often usual that attackers unknown of the network layout will listen to the traffic to build a map and find weaknesses of the network [Panko, 2010]. This is also very dangerous if passwords and other authentication details are passed on the network.

4.4.3 REVERSE ENGINEERING OF COMMUNICATION PROTOCOLS

Eavesdropping is not possible on all networks, since undocumented, secret protocols might be used for data communication. However, if the protocol does not contain

decryption, an attacker might attempt to reverse engineer the protocol to be able to extract sensitive information out of the traffic [Homeland Security, 2009].

4.4.4 MAN IN THE MIDDLE

Man in the middle attacks is potentially the greatest threat against a security system at this tier. Using different techniques, exploiting the fact that many fundamental network protocols does not have built in security, an attacker can make two devices believe they talk to each other while the attacker intercepts and potentially modifies the traffic (seen in illustration 9). A successful attack can provide devastating since the security system might look fully operational but alarms will not get through, the cameras might show old play backs of video, doors might report status unlocked, but the guard will only see status locked etc. Simple encryption will not always be effective against this attack. The man in the middle might also inject arbitrary traffic, such as shutting down alarm zones and unlocking doors. [Homeland Security 2009].

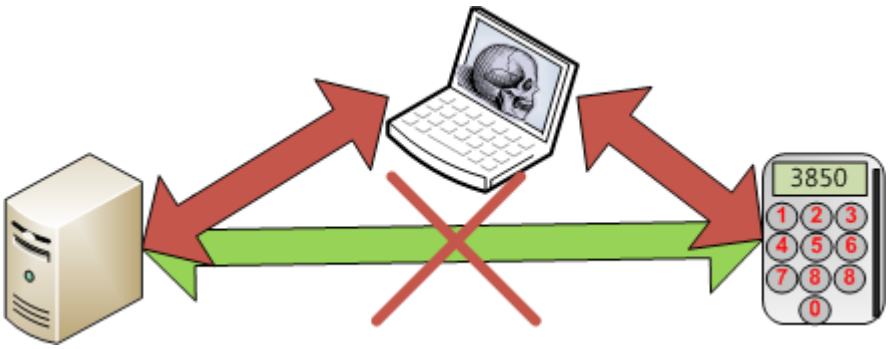

Illustration 9: Man in the middle. One attacker captures traffic between two devices and effectively controls the system

4.5 TIER THREE – DEVICES, CONTROLLERS AND APPLICATIONS

Threats at this tier threaten the operation of the system and it functions. The vulnerabilities varies depending on the system implementation. This reflects threats against an integrated security system on more generic level. The goal of the attacker is to gain access to the system and operate it. This might be devastating, since illegitimate users might get access in the door access control system and alarms and video surveillance might be disabled or recordings deleted.

4.5.1 AUTHENTICATION VULNERABILITES

The process of verifying that the user is authentic is vital to a security system. An attacker might attempt to use account with easily guessed passwords. This specifically applies to integrated security systems where many passwords are numbers only. This is the case since a lot of the edge devices requires digits as input from a simple control panel to open doors etc.

An attacker might also try default system accounts, that is pre-installed and might give the attacker full control over a system. Another vulnerability in systems that misses a centralized user manager, is that accounts of ex-employees might still be left in the system for a long time before they are found [SEMA, 2008].

4.5.2 OPERATING SYSTEM EXPLOITS

One common way to take control over an application is to exploit vulnerabilities in the underlying operating system. If the operating system is not hardened, there might be services and vulnerabilities that an attacker can use. If the underlying system is compromised, it is very hard to protect the application [SEMA 2008].

There is also a possibility of malicious code, such as viruses and trojans, getting into the operating system. Malicious code can expose the system with critical vulnerabilities and cause damage on the system [Pfleeger, Pfleeger, 2007]. Integrated security systems are less vulnerable to viruses and trojans than administrative IT systems, since they do not usually run e-mail and Internet software that is large source of malicious code. However, the threat is there none the less. Malicious code can find its way into via USB sticks and bad user behavior.

4.5.3 APPLICATION INSECURITIES

At the point the user accesses the applications within an integrated security system, network and operating system access must have succeeded. There is still a threat, since users inside an integrated security system may have different privileges in the system. Guards might only be able to see the alarms while the security officer can enable and disable the system if needed [Norman, 2007]. The threat is about users wanting to raise their privileges in the system to access unauthorized features. There can be a lot of different application specific flaws in an application. This study does not really cover the design of software application but rather the architecture of the installation. The most common attack against applications with databases is SQL injections [Pelliccioni, et. al. 2008]. This is a common method of attack and is often successful since a back end database might not always have fine grained access control to its stored data. This access control is usually done by a front end application server. By fooling the front end to send malicious SQL queries to the back end database, the attacker might gain unauthorized access to the system [Pfleeger, Pfleeger, 2007].

5 STANDARD AND GUIDELINE ANALYSIS

There are several standards and guidelines to design IT architecture around. However,

most of them target very specific system setups and usage scenarios. This is an attempt to analyze a few of the guideline documents that influences the Swedish market. The analysis will be in respect to how well they apply to the security threats and risks of integrated security systems.

5.1 SELECTION

Three standard documents have been chosen to be included in this study. There is no widely used standard or guideline documentation for IT security within integrated security systems specifically. The guidelines chosen represent digital control systems in general as well as more standard administrative IT systems. The selection of these specific standards is provided by Peelit AB as a foundation to construct the secure architecture. Each document is referenced by an abbreviation to increase the readability. The documents are listed below.

5.1.1 BITS

Basic level for information security (BITS) is a Swedish standard for base level IT security that governmental agencies must fore fill. It is based on SS-ISO/Iec 27001 [SEMA, 2006].

5.1.2 CSRP

Control Systems Recommended Practices. It is a set of documents in the Control Systems Security Program (CSSP), United States Computer Emergency Readiness Team, which is a part of the U.S. Department of Homeland Security. The analysis will focus on the document “Improving Industrial Control Systems Cyber-security with Defense-in-Depth strategies”, since it is the document giving guidelines for IT security in an architectural point of view. However, some of the other documents within CSRP will be references when addressing specific system details [Homeland Security 2009).

5.1.3 NIST SP800-82

Guide to Industrial Control Systems (ICS) Security by National Institute of Standards, U.S. Department of Commerce. The document includes practices that companies and organizations related to the U.S. market is recommended to follow [Stouffer et.al, 2008].

5.1.4 MSB

Guide to Increased Security in Process Control System for Critical Societal Functions, Swedish Emergency Management Agency. This is the recommended guidelines by the Swedish authorities to implement security in digital control systems [SEMA, 2008].

5.2 ANALYSIS OUTLINE

This study is only includes the system architectural parts of each standard/guideline document. Parts of the documents that is of organizational and/or process nature is not in the scope of this study. For each document, the analysis will first target the intended usage and audience for the document. Then an analysis is made on how the document addresses each of five selected topics with respect to the threats and risk analysis previously made in this report. The major focus is to find obvious threats and risks not addressed and find parts that are not applicable to integrated security systems in general. The five topics are

- Network segmentation
    - How segregation of network segments with different security requirements is handled.
- VPN Access
    - How VPN access security is treated in the system
- Machnine-Machine communication
    - How is communication between devices with no user input treated?
- Backdoors
    - Other ways to access the system other than through the main firewall.
    - This can be modems, wireless networks and other communication equipment that can be used as a backdoor into the system.
- Application Security.
    - This deals with different aspects of application authentication and application security.

5.3 ANALYSIS OF BITS

5.3.1 ABOUT BITS

The document is written by Swedish Emergency Management Agency. The standard gives a set of guidelines and rules how to achieve a base level of information security within IT systems. The document is aligned with the Swedish standard SS-ISO/IEC 27001. The guidelines are aimed towards key organizations in the society to be able to function even under stressful social disruption. This document can be used as a template to implement the standard SS-ISO/IEC 27001.

BITS addresses all parts of processes that is needed to create a secure information system. This includes planning, information management, system architecture, operations, maintenance and the behavior of the users in the system.

The architecture of BITS is a relatively comprehensive model for IT systems. All pieces from access, networking, via the operating system to applications and information systems are covered. BITS puts a lot of effort in authentication of users in different stages. This is specifically the case of strong passwords and login management.

5.3.2 NETWORK SEGMENTATION

The network perspective in BITS is focused around one central point – the firewall, which is seen as central resource that should cover the network security needs for the entire company [MSB, 2006, p. 48-49]. As a response to the major importance that is given to this only way in to the system, a set of counter measures is proposed to secure the firewall. Among others, intelligent anti-virus functions is proposed. Network segmentation and defense-in-depth is only partially discussed. This can be somewhat difficult with integrated security systems, as proprietary protocols are is often used, which limits advanced firewall features such as deep packet inspection and anti-virus scanning [Byres et. al, 2005]. Also, CCTV systems often uses huge amount of bandwidth that very advanced firewalls and gateways might have problems with.

5.3.3 VPN ACCESS

There are very few guidelines for distance work and VPN tunnels. BITS only points out that anti-virus protection, authentication and physical equipment protection has to be considered. No architectural guidelines are given for VPN clients and other distance connections. This is unfortunate since remote access to operate the security system is an integral part of this study. Specifically setups like split tunneling on the client is not

considered. That is, it is essential for the security of an integrated security network to not let remote clients route illegitimate traffic into it. In this case, BITS does not cover the needs for integrated security systems.

5.3.4 MACHINE – MACHINE COMMUNICATION

Secure communication between machines where no user does authentication is not a part of BITS. As it is as central perspective in digital control systems, specifically integrated security systems, where there are a lot of equipment communicating and few users. Illegitimate equipment that tries to be a part of the network can prove devastating.

5.3.5 BACKDOORS

WiFi, 802.11, networks are covered as back doors that will need additional protection in chapter 11.4. WEP, Wired Equivalent Privacy, is proposed as security solution. At the same time, BITS states that WEP is not the entire solution, and needs additional security. Today, however, WEP is totally outdated and attacks that could break WEP within minutes was published already 2004 [KoreK, 2004].

5.3.6 APPLICATION SECURITY

When it comes to application security from a user perspective, BITS has a lot of good practices and guidelines. Authorities should be based on a need-basis and administered from a central system, accounts should be locked after three failed login attempts and passwords needs complexity and should be changed regularly is some of the guidelines described in BITS. These are of course good practices in general, but in physical security systems, sometimes the passwords has to be handled on small keypads with only digits which makes complex passwords hard to implement. Another feature is that accounts should be locked down after failed attempts: that is not really an option since high availability is, as stated earlier, of more importance than security.

5.3.7 ANALYSIS SUMMARY

BITS takes the security from a user perspective rather than from an attacker perspective. Also given that the target for this standard is administrative it systems rather than digital control systems, which gives many differences in assumptions about the target system capabilities. Routines to create a defense-in-depth approach is missing and security around remote access are not widely discussed. However, the parts about application security will well adapt to the it-system part of an integrated security system.

5.4 ANALYSIS OF CSRP

5.4.1 ABOUT CSRP

The documents purpose is to create routines and understanding how digital control systems can securely exist side by side with administrative it systems using defense-in-depth strategies. The document is biased towards network security rather than application security or procedures. The architecture in the document is based on a layer perspective with an external zone, internal zones such as office networks and then different layers of the control system network based on sensitivity of the systems. The main idea is that all networks and VPN connections is segregated with internal firewalls. On top of that is a layer of IDS systems that raises alerts on intrusion attempts.

5.4.2 NETWORK SEGMENTATION

Network segmentation is mostly what CSRP is all about. The document gives very deep guidelines on how to dive a corporate network into zones that corresponds to different security levels. The zones are based on the layer architecture where inside zones are locked down with firewalls. This setup seem to fit the way integrated security systems are organized and can be located inside the corporate network with no access to external networks such as the Internet.

For semi-public devices, one or more DMZ is proposed for each zone. For integrated security systems, that would mean that devices that are connected to the outside world, such as VPN gateways, modem connections etc. can be placed within a DMZ to protect the other parts of the security system.

There are a lot of recommendations about firewalls of different types to be customized for local parts of the system. One example is “plug-n-play” firewalls to connect directly to controllers and end equipment that cannot use software based firewalls. This concept is interesting to minimize exploitation on critical equipment. Defense-in-depth refer to another document, NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks [Byres et. al., 2005]. This document gives a lot of important guidelines for digital control systems. Especially guidelines on how not to do are well needed in the firewall design for integrated security systems.

5.4.3 VPN access

External connections for remote control or for connection between multiple physical locations to one logical network are an important part of IT security in integrated security systems. CSRP solves this by proposing VPN connections to be terminated into a DMZ

where the firewall can be configured to only allow access that is needed by the user. More detailed information about how this configuration should be setup is not given, but that is probably project and vendor specific.

5.4.4 MACHINE – MACHINE COMMUNICATION

The integrity in an integrated security system is a vital factor. It is of great importance that the monitoring system communicates with the correct device and gets correct alarm signals and status updates. At this point, CSRP does not cover handling of possible illegitimate equipment much at all. IDS detectors are proposed to be placed in virtually all firewalls, to discover attack signatures and odd behavior. This can be a good mechanism to monitor the integrity of a physical security system, however, the IDS on the market is not optimized to find attack signatures in the proprietary protocols used in physical security systems. The work on digital control systems and SCADA has come a bit further, where ICS protocols are integrated into many IDS systems. Some of these protocols are used in physical security systems as well, such as modbus. [Peterson, 2007].

There are warnings about man-in-the-middle attacks, but no architectural solution to that problem is presented.

5.4.5 BACKDOORS

A potentially serious backdoor into integrated security systems is through modem connections that is used to send alarm and status reports to security companies, security centrals etc. CSRP provides detailed information on how to secure modem connections in a whole document [Homeland Security 2008]. This information contains practices in encryption, dial-back and the usage of DMZ to protect other resources from vulnerable modem connections among other ideas.

The other major backdoor, wireless LAN, is also covered. WPA2 with AES encryption is proposed while also noted that it cannot be used alone without other security mechanisms. The summary is that WLAN networks should be considered insecure networks and the network architecture should be built accordingly. That is, in critical systems, WLAN should be avoided.

5.4.6 APPLICATION SECURITY

Although CSRP does not cover much application security, a few common threats are covered.

- SQL Injections – might give an attack way from less secure databases in the

corporate LAN into critical databases in the digital control system past all firewalls.

- Unpatched systems keep known vulnerabilities.
- “Secret”/proprietary protocols that might even be in plain text/ascii are easy to reverse engineer for an attacker.

When it comes to core application security such as authentication, then some supplementary standard is needed. For instance BITS.

5.4.7 ANALYSIS SUMMARY

In most cases, CSRP is applicable to integrated security systems that are considered in this study. Even though CSRP is written toward ICS of the type that exists in factories and plants, there is a lot in common with integrated security systems. A few topics need to be translated into the context of security, though.

5.5 ANALYSIS OF NIST SP800-82

5.5.1 ABOUT NIST SP800-82

The Guide to Industrial Control Systems (ICS) Security by the U.S. National Institute of Standards and Technology is a standard document for it-security within ICS and SCADA systems. It is used as a basis to reach minimum requirements of security for federal agencies and voluntary by other organizations and companies. NIST SP800-82 takes stand in different scenarios and proposes architecture for increased security.

5.5.2 NETWORK SEGMENTATION

Segregation between the control system and the corporate network is proposed as an absolute minimum. One or more DMZ is recommended between the control system network and the corporate network. Exposed servers that need to be accessed from both networks are then placed within a DMZ. This applies well to the system considered in this study where the integration server needs to accessed remotely. The requirements for firewalls between the control system network and the corporate network are well specified. The essence is that incoming traffic should not be allowed and outgoing traffic should be restricted to the services (destination IP address/port) needed.

5.5.3 MACHINE – MACHINE COMMUNICATION

If the network is kept relatively static, which is often the case in integrated security systems as in other digital control systems, static ARP tables and port to MAC lock is proposed on switches. That will make it difficult for non-authorized equipment to communicate in the network. As a long term, high end, solution, complete encryption and authentication between devices is proposed. This solution will prevent eavesdropping and MITM attacks as well as traffic injections and modifications. SP800-82 covers most things that are needed in this area.

5.5.4 VPN ACCESS

SP800-82 recommends VPN technology for remote access to control system computers and for inter site transit. IPSec, SSL and SSH are presented as technical solutions.

5.5.5 BACKDOORS

SP800-82 applies rather strict policies on WLAN connections. The most important ones is that WLAN devices should connect to a separate network with limited access to the control system network. Minimum security requirements on the WLAN is that encryption is enabled, connections is limited to predefined MAC addresses and SSID broadcasting is disabled. In terms of detailed information on how to secure a wireless LAN, SP800-82 refers to another standard by NIST: “Establishing Wireless Robust Security Networks”, that covers a lot wireless security aspects. This approach suits integrated security systems. If there is a need for WLAN, then it should not have direct access to the security system.

The standard does also provide security guidelines for communication with modems. Strong authentication, encryption and auditing of usage is recommended. Dial back is also proposed as a very basis, although that is not a complete solution. SP800-82 goes so far that it recommends turning off modems when not using them. However, this is not a possibility for integrated security systems which are supposed to be operational 24/7.

5.5.6 APPLICATION SECURITY

SP800-82 considers application security, at least in the context of application layer protocols. To limit the possibility for trojans and viruses to create a tunnel out to the internet from the control system network, usage of insecure protocols is discouraged on both sides of a DMZ. Examples of insecure protocols would be HTTP and modbus. The

recommendation is then to use, for instance, HTTP from the corporate LAN to the DMZ and modbus from the DMZ to the control system. This recommendation is valid, but a lot of vendor specific equipment in integrated security systems uses HTTP of some sort, so the implementation of this practice might need workarounds.

Anti-virus software is recommended to be installed on all main stream operating systems (Windows, Unix, Linux), both servers and workstations. The standard clarifies that anti-virus and software patches should only be used if it has been tested and known to not cause performance and reliability problems. The performance is specifically critical to the CCTV part of integrated security systems, which requires heavy real time computational power to perform video analysis [Norman, 2007].

5.5.7 ANALYSIS SUMMARY

SP800-82 addresses pretty much all the field of risks and threats against integrated security systems. Everything from network segmentation to back doors, authentication and malicious software is covered. Several references to other guideline documents is provided for more detailed information about areas like encryption, secure wireless connections etc. References to the defense-in-depth document from CSRP is also included to cover up details around network architecture and defense-in-depth strategies.

5.6 ANALYSIS OF MSB

5.6.1 ABOUT MSB

The document, Guide to Increased Security in Process Control Systems for Critical Societal Functions, is developed by Swedish authorities in cooperation with major Swedish organizations and corporations. The purpose of the document is to increase the awareness and need for security within process control systems. The guidelines are on a fairly high level and covers mostly processes and organizational matters, rather than architecture. However, it is included here since it is important on the Swedish market.

5.6.2 NETWORK SEGEMENTATION

MSB recommends separating the process control network from the administrative network, as much as possible. There is also a recommendation about separating the process control network into several zones depending on the sensitivity. External or insecure connections should be placed inside DMZ zones. There are, however, no more details about how to build the architecture. Rather, a few references are supplied. Although brief, the guidelines seem to fit well into integrated security systems.

5.6.3 MACHINE – MACHINE COMMUNICATION

The integrity of communication between devices in the network is not covered on a cryptographic basis. However, other counter measures are provided, such as IDS systems scanning for unusual network activity. Physical protection of equipment is also suggested. This is of course possible for process control systems, but that physical protection is a part of an integrated security system. Physical protection is not an option here, at least not for the edge devices such as CCTV cameras and card readers. The servers and controllers can be kept protected.

5.6.4 VPN

MSB only notes that remote access requires special considerations, strong authentication should be used and the method and computers that can be used for remote access should be restricted. The recommendations are very brief, but do not contradict the implications of an integrated security system.

5.6.5 BACK DOORS

The document confirms that many process control networks contain back doors such as wireless networks, modems, ISDN and bluetooth. The only guideline is that the connections should be identified and equipped with security mechanisms. This is very vague, and does not reflect the level of security that is in the scope of this study.

5.6.6 APPLICATION SECURITY

MSB covers application security such as hardening of applications. Examples are given on application hardening such as changing factory settings, enable the best possible security and turn off unused features. It is also stated that hardening often requires the manufacturer to provide hardening guidelines to not have operational disturbances. The guidelines are wise, but too brief to be usable as an architectural guideline.

5.6.7 MBS SUMMARY

The guidelines do not put much focus on architecture. The architectural guidelines that are given are in many ways too brief to be usable directly. Although, most of the guidelines are relevant for integrated security systems, supplementary guidelines with more details should be used. Then it is good that MSB provides such relevant references.

6 SYSTEM HARDENING ARCHITECTURE

6.1 ABOUT THE ARCHITECTURE

This is the proposed architecture, which is based on the security standards presented and analyzed earlier.

6.2 NETWORK ARCHITECTURE

6.2.1 GENERAL NETWORK HARDENING

There are some techniques to harden a network that are rather generic but applies well to control system networks and hence security systems. Since the edge devices are rather exposed to the surrounding, it is essential to make it hard for anyone with unauthorized network access to communicate on the network. These steps are not really possible on a network that changes often but that is not the case of an integrated security system.

Switch ports should be locked to the MAC address of the connected device. This way it is harder for an intruder to connect alien devices on the network, at least without notice [Stouffer, et.al. 2008]. This method is recommended by sp800-82.

DHCP should be disabled on all devices in the network. DHCP can be used by an attacker to reorganize the network and make it insecure. Fake DHCP can broadcast malicious network settings which can make way for MITM and DoS attacks.

Preventive measures against ARP poisoning should be taken on particularly sensitive network segments. This will make it harder for attackers to complete a MITM attack. Measures include static arp tables and special software. Note that this measure requires extensive work on a large network and that not all devices (such as embedded cameras, card readers etc) allows detailed configuration. This approach, however, allows for extra security where needed and is recommended by SP800-82.

6.2.2 SEGMENTATION

The architectural approach used in CSRP [Homeland Security, 2009], where the devices of the control system network are segmented into different zones based on the level of sensitivity, will be used as a basis. Systems that are accessible by remote users or machines on other networks should be placed in a DMZ based on the two firewall dmz design, described in the standards. The major parts of this approach are also recommended by MSB [SEMA 2007] and SP800-82 [Stouffer, et.al, 2008].

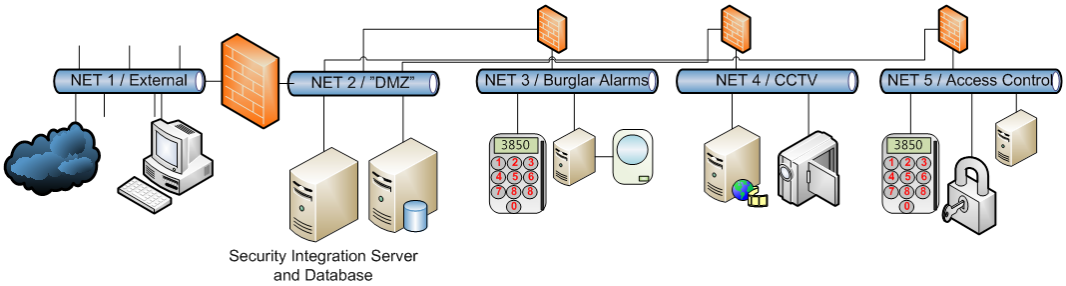

Illustration 10: Segregation of sub systems with firewalls

Some differences have to be made to implement this architecture on an integrated security system. The primary factor is that it is rather hard to classify security systems as more or less sensitive on a generic basis. This classification will be specific for each installation and the purpose of the installation [Norman, 2007]. Since all integration between the physical security sub systems will take place in the integration server, all communication between the sub systems should be denied. A naive approach is presented in illustration 10. This approach works well, since all external communication has to be directed to the integration server which handles the communication with the sensitive sub systems. Each firewall should be configured to only allow communication between devices that needs it.

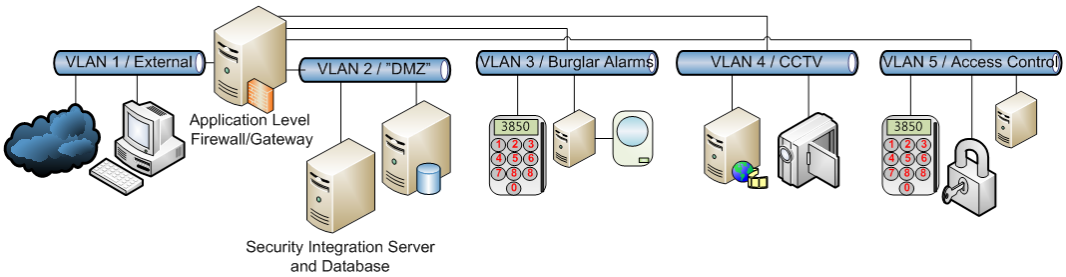

Illustration 11: Network segregation using VLAN and one firewall/gateway applying firewall rules in software on each VLAN.

The architecture in illustration 10 is awkward to implement. It requires separate network hardware and cabling for each network. It also uses several firewalls that needs configuration. Using VLAN (IEEE 802.1q) and a firewall that can apply firewall rules according to the corresponding VLAN id, it is possible to allow the same security setup but with nearly the same amount of hardware as if there is no segregation at all. The proposed setup is in illustration 11. Each sub system resides on its own VLAN. The central integration server has also its own VLAN. This allows a backbone network with a single group of switches to provide segregated network communication over the whole area of the facility. A camera can physically share the same switch as the integration server, for instance.

6.3 APPLICATION LAYER GATEWAY ARCHITECTURE

6.3.1 DEFINITION

The application layer gateway is a key concept in this approach. The term, application layer gateway (AGL), might be a bit misleading, and does not reveal the whole concept of this device. Do not confuse this terminology with the one defined in rfc2663 [Srisuresh, P.; Holdrege, M, 1999]. The definition of the device used in this setup (can be seen as requirements as well) is:

- An AGL is a VPN server using an inherently secure encryption protocol such as SSL, SSH or IPSEC
- The VPN server should have a client/server architecture that allows access only if the client host has valid security features enabled (firewall, anti-virus etc.).
- The AGL should provide user/password for the authentication process that should be possible to connect to an authentication service.
- Each user should have an individual ACL, which limits the user to connect to authorized hosts/ports.
- The AGL should be able to route between VLAN with ACL firewall rules controlling the routed traffic.
- The AGL should be hardened to withstand Internet exposure.

Notice that there is no particular requirement that the AGL understands the underlying protocols.

6.3.2 CONFIGURATION

Assuming the setup shown in illustration 11, the following rules should be configured in the AGL.

Rule	**Comment**
Traffic to and from VLAN1 from any other should be denied. Except from traffic to the VPN port at the AGL.	All traffic to and from the Internet and other external networks has to be through authenticated VPN connections.
VPN users should be setup with profiles that specifies their needs. Normal users to access the integrated systems and various administrators that represents the technicians who administer the different sub systems.	This corresponds to access on the least privileges basis that is proposed by BITS.

The user profiles should be handled in a centralized user management system. The passwords should be complex.	
VPN clients need to have sufficient protection available to connect. Specifically no split tunneling should be allowed.	This can prevent malicious code from creating a connection from an attacker via an infected VPN client host to the security system.
Traffic from VPN clients to VLAN2-5 should be authorized according to need. A normal user should only be allowed to access the application specific ports on the security integration server at VLAN1. Administrators should have access to whatever system they are responsible for. This should be administered in the user profile access rules.	This implements network access restrictions. Specifically a normal user will only have access to the applications he need to access on the specific hosts he needs. This is effectively an implementation of a DMZ-like zone. In the basic case the access is limited to the integration server service. In other administrative cases, the access should probably be done under controlled circumstances, such as locally. This setup also implements the ideas of the Collaboration Open Framework by Jericho Forum – the ideas of de-perimeterization [Olovsson, 2006].
Traffic from sub system VLANS (VLAN 3-5) should only be allowed to the “DMZ”, (VLAN 1). Specifically access should only be permitted to the needed ports on the integration server. Make sure that the ALG routes between the VLAN´s as well.	This implements network segmentation according to CSRP, SP800-82 and MSB. The implementation is in software instead of hardware. A resilient and hardened ALG is recommended.
Traffic from the DMZ (VLAN 1) to the sub system VLANs (3-5) should be allowed to devices that communicate directly with the integration server. On some systems, this might include the edge devices such as cameras, but on other systems only centralized controllers or servers might need traffic.	This implements the final step in the DMZ zone. Only limited traffic should be going to the DMZ.

6.3.3 IMPLEMENTATIONS

The AGL defined in this text can be implemented in a number of ways. I will not present any implementation specific details or list all vendors that offer this product, since it is not in the scope of this study. To prove this approach to be useful in practice, two example product that offers this functionality is presented. Note that the two products are not chosen of any particular reason other than that I had a chance to test them and verify the required functionality.

The AppGate Security Server is an application layer firewall by AppGate. It offers VPN through SSH and SSL. Verification software is possible to run on the client to allow or deny VPN connections. Authentication can be done with radius, LDAP etc. VLAN is supported with firewall rules. [AppGate, 2010].

The Cisco Adaptive Security Appliance 5500 is a security appliance by Cisco. It supports VPN trough SSL and IPSEC. Users can be authorized by radius and system client protection can verified before a VPN connection is established. It supports VLAN with firewall rules [Cisco, 2010].

6.4 CLIENT NETWORK ACCESS

The various standards (specifically CSRP) specifics the control system network according to a local administrative IT network (corporate LAN). In this architecture, a local administrative IT network is not a requirement. This architecture should be applicable on facilities without on-site personnel or IT systems, such as outdoor perimeter surveillance. A client on a local administrative IT network will be considered as any client connecting from the Internet. Since the security is kept high on integrated security system itself, no further consideration has to be taken when for instance out sourcing the security management of a facility. That said, it is a security advantage to keep the clients used to access the security system in a locally connected network that already have some security.

6.4.1 CLIENT HARDENING

The client host connecting to the system needs to be hardened. Even though the access of the client is very limited on the security system network, it is important that the client does not become a back door into the security services. A remote client host will be a part of the perimeter defense of a network, so the protection is important [Olovsson, 2006].

These steps needed to harden a client operating system is very much dependent on each specific case. Most modern operating systems have security baseline documentation that can be used for detailed instructions. In general the hardening process for an operating system includes changing default passwords, remove unnecessary programs and services and install patches that fix security issues [Panko 2010]. It is also important to add software firewall to the host. The firewall should reject any traffic that is not to or from the security system. Specifically, the client should not have more than one external connection, to avoid problems the dual homed hosts specified in SP800-82 [Stouffer, et.al. 2008]. External connections could multiple ethernet connections, bluetooth connections, wireless (IEEE 802.11) connections, mobile broadband (such as GPRS/UMTS/HSPA/LTE) etc.

Client hardening also includes hardening the security client software that is used to connect to and control the integrated security system. This is very software specific, but can include enabling encryption and making the program accessible only to a specific user on the computer. Consider looking at the security baseline for the client software of the specific product.

6.4.2 OTHER REMOTE SYSTEMS

Other remote systems may need to be connected. For instance integration with alarm centrals through TCP/IP, modems etc. [Norman, 2007], [SEMA, 2008]. To keep the system security intact and avoid dangerous back doors, such integrations should be done using the front door VPN access using the official security client to connect to the integration server itself. To keep the security at a really high level, other integration should be avoided. It is not in the scope of this study to present solutions for this kind of integrations. However, if modem connections or other back door connections are needed, the network segregation already proposed together with additional security measures [Homeland Security 2008] for the external connection will help securing the network.

6.5 SERVER SYSTEM HARDENING

6.5.1 AUTHENTICATION

The use of a central, harden authentication system is important. This allows all authentications to be made in a secure fashion that is easy to administer. The implementation of this authentication system can be as a service on the integration server, the AGL or a separate server in the DMZ network. There are several standards for authentication systems, such as RADIUS and kerberos. This approach results in role based access that is easier to manage if there is many users in the system. The best practice is to use the same authentication system for all layers. That is, for the network access, the operating system access as well as the application access. The authentication system can also be used by the sub systems, such as the CCTV servers, if appropriate.

6.5.2 OS HARDENING

Hardening of the server operating system is critical. If the server is taken over the services it offers might also be exploited. In this case, access to the physical security system. In general the hardening process for a server operating system is the same as for hardening of a client OS. This includes changing default passwords, remove unnecessary programs and services and install patches that fix security issues [Panko 2010]. Schemes for hardening of specific systems are usually offered by the software vendor. The U.S.

National Institute of Science and Technology offers a list with up to date security baseline documents for common operating systems at this URL http://web.nvd.nist.gov/view/ncp/repository.

In this specific case, the server should only offer the services needed by the security system server software. This includes a database server and authentication services if they are run on the same physical server. A host based firewall should be installed to fully utilize the defense-in-depth strategy recommended by CSRP. This firewall should only allow connections to the specific services offers from the other systems that uses it. This decreases the risk that attackers can exploit unknown vulnerabilities in the OS or the software running on it.

6.5.3 DATABASE HARDENING

Database systems in general can be hardened like other software. General actions are to provide centralized authentication, remove default accounts/passwords and enable encryption, if it is supported. Specifically, with a centralized authentication system, the integration server software accessing the database does not have to store a password in a configuration file somewhere [Pfleeger, Pfleeger, 2007].

It is also important that the accounts used by the integration server to access the database use the least privileges principle. This will make it harder for an attacker to exploit vulnerabilities in the application and execute SQL injections [Pelliccioni, 2008].

6.5.4 APPLICATION HARDENING

Most of the vulnerabilities in the application layer is based on bugs in the software itself, or bad configurations. At this point, it is really important to choose integration software that has a high level of security, since such things cannot be fixed afterward easily.

SQL injections can be used in the client software to gain more access than authorized. This sort of vulnerabilities cannot be mitigated in a good way at the application layer, without modifications on the software. It requires the attacker to have access to the software itself and the database hardening should provide some protection [Pelliccioni, 2008]. Still, it is important to be aware of this risk.

6.6 SUB SYSTEM AND EGDE DEVICE CONSIDERATIONS

Even though detailed hardening of the sub systems are not part this study, a system is no more secure than its weakest part. Therefore, it is of great importance that hardening of the internal architecture of each sub system is done correctly.

6.6.1 CCTV CONSIDERATIONS

CCTV installations can alone be large and complex systems. The primary architecture does, for instance, not allow client PCs to connect directly to the CCTV servers. In some cases, it might be necessary to allow clients to connect directly to the CCTV server. It is important that this connection is done through the ALG the same way other client connections are made. The user accessing the video stream from the CCTV server should only have access to the specific services on the specific hosts on the CCTV VLAN.

As noted previously, it is important that access to the network equipment is not physically possible for unauthorized persons. IP cameras are particularly exposed since they often reside on the outside of buildings. Analog cameras connected to an analog-to-digital video encoder in a secure place will prevent an attacker from physically connect to the security network by physically control an IP camera. This, of course, has downsides as well since the benefits of IP communication cannot be used. However, this is still an option.

6.6.2 BULGAR ALARM CONSIDERATIONS

Bulgar alarm systems are often quite simple with respect to the computer/network-connection. However, if the system supports encrypted communication or other means, such as call back, to provide increased integrity, that should of course be enabled. These systems often contain external communication through dial-up or ISDN. This is a security risk since the external connection can be exploited, and if really needed, as noted before, there are standards how to harden such connections.

6.6.3 ACCESS CONTROL SYSTEM CONSIDERATIONS

As with IP cameras, card readers and key pads in access control systems can feature direct IP connectivity. This exposes the security network to an increased risk since the card readers are easy to access and cannot often be locked in. When installing the access control system, not only the security of the access control system, but the entire security system has to be considered, when hiding the wires and other things.

7 CONCLUSIONS

7.1 ANALYSIS CONCLUSIONS

The analysis of the cyber threats that might be directed towards integrated security systems shows that there are all the threats normally found in administrative IT environments, but with the difference that many of the devices that forms the integrated

security system is not physically protected – but instead used to protect other sensitive assets. The number of legitimate users on the system can be considered low, so threats that are very common on the internet, such as SQL injections, are not as big threat towards security systems. Given the threat environment, security systems are often built with embedded devices that are very immature in using TCP/IP and have yet to discover many of the security holes and issues that has been dealt with in the modern unix/windows/linux world.

The big downside with the standards in the area is that there is no good standard documentation or guidelines for security systems at all. Since integrated security systems are categorized as industrial control systems, these standards apply in theory. They are good at handling the architectural and security aspects of process control systems and other kind of industrial control systems but fail to apply to the context of integrated security systems. The main difference is that industrial control systems used for process control etc. features heavy integration with the administrative IT network, but can be physically protected from unauthorized persons. The integrated security system cannot be protected to the same extent, but does not need the same amount of integration with the administrative IT system. Specific guidelines and cyber security standards are really needed since security systems become more and more connected to IP networks. It is a matter of security for assets and people.

7.2 HARDENING ARCHITECTURE

As could be seen in the threat analysis part, threats against the availability of the system are the most dangerous, since availability is critical to security systems. There is no explicit method to provide hardening against DoS attacks suggested in the standards. The architecture proposed provides implicit protection against DoS attacks by segmenting the network into strict zones. Since traffic cannot flow between the zones except between explicit stated end points and client PC:s will not be directly connected to the network other than authenticated and encrypted through the gateway, an attacker cannot easily direct DoS attacks in the network. An attacker can possibly only affect the VLAN which he have gained access to. That said, the final defense against availability threats is of course robust and hardened software and hardware implementations, but this hardening architecture really helps.

For complexity, the architecture is really good as there is very little overhead in hardware and software. The ALG and VLAN switching is all that is required, so this solution can be used in many cases. Since extensive configuration of access rules is required, this solution takes a lot of work if the installation changes dynamically over time. Hence, a rather

static environment will best fit the architecture.

One thing worth noticing is that I do not presume any difference in security sensitivity in different parts of the sub systems. For instance, one set of cameras installed in a top secret development facility that should be accessible only by special guards and one set that is used to monitor the car parking. Such segregation is not considered in this study and the possibility to modify the architecture to handle that case is not known. In this case, the proposed architecture is flat and the security does only depend on the internal software security of the integration server.

As a final conclusion, it is possible to harden an integrated security system to withstand most of the threats or at least make it not worth the cost to break the IT security of the physical security system. As in all security critical systems where humans are involved, the main factor of mistakes is the human.

7.3 FUTHER STUDIES

This study only concerns homogenous physical security systems with integration to specific monitoring PC clients. In cases where the security system needs integration with other digital control systems, such as lights, heating, lifts, generic building automation, process control SCADA system etc. then this security model might need to be changed. This also applies to security systems that need heavy integration with administrative IT servers or even exposed web based services.

An overall security architecture like this does increase the security of the overall system. However, hardening processes for sub systems like CCTV, access control and bulgar alarm should be needed. This is an upcoming factor when it comes to CCTV, since more and more recent technology starts to become wireless. This might need a whole different attention on the security aspects of each sub system as the exposure increases.

The architecture is also not the major factor when comes to security. To keep the maximum level of security, usage patterns, auditing processes and incident management an d response is really important. Guidelines for this kind of processes when it comes to cyber security in integrated security systems should increase the overall security by far.

GLOSSARY

ACL	Access Control List – rules that specify firewall access rules.
CCTV	Closed-Circuit Television, surveillance camera systems
ICS	Industrial Control System
IDS	Intrusion Detection System (computer intrusions)
IPSEC	IP Security – A standard for encryption of ip packets on the network layer.
ISP	Internet Service Provider. Provides Internet access.
MODBUS	A generic protocol used in automation and industrial control systems
TROJAN	A malicious program
SCADA	Supervision Control and Data Acquisition – A class of software that monitors and controls industrial control systems.
SSH	Secure Shell – Encrypted remote shell access and tunneling protocol.
SSL	Secure Socket Layer – Encrypted Application layer protocol
VLAN	Virtual Local Area Network. Several logically separated networks using the same cables and switches.
WLAN	Wireless Local Area Network, WiFi, Wireless Local Area Networks.

REFERENCES

Barret, D.; Silverman, R.; Byrnes, R (2005): *SSH, The Secure Shell: The Definitive Guide*, 2:nd edition, Sebastopol: O´Reilly Media

Byres, E., Karsch, J., Carter, J., (2005), *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* Revision 1.4, Brittish Institute of Columbia. Available online: http://www.cpni.gov.uk/docs/re-20050223-00157.pdf [Accessed 2010-03-31]

Cisco (2010), *Cisco ASA 5500 Series Adaptive Security Appliances.* Product Data Sheet. Available online: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html [Accessed 10.05.03]

Fielding, R. et. al., (1999). *Hypertext Transfer Protocol, Request for Comments 2616.* Available online: http://www.ietf.org/rfc/rfc2616.txt. [Accessed 10.03.31]

Fleisch, Brett, (2003). *Grand Research Challenges in IT Security and Assurance*. Available Online:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.9931&rep=rep1&type=pdf [Accessed 10.05.07]

Habib, Sheikh Mahbub; Cyril, Jacob; Olovsson, Tomas (2009): *An Analysis of the Robustness and Stability of the Network Stack in Symbian-based Smartphones*. *Journal of Networks*, Vol 4 (No. 10, 2009) pp. 968-975. Available online: http://publications.lib.chalmers.se/cpl/record/index.xsql?pubid=102441 [Accessed 10.4.29]

Henmi, Anne. (2006) , *Firewall Policies and VPN Configurations*, Rockland: Syngress Publishing

Homeland Security, (2008), *Recommanded Practice for Securing Control System Modems.* http://csrp.inl.gov/Documents/SecuringModems.pdf [Accessed 2010-03-10]

Homeland Security, (2009), *Recommanded Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.* Available online: http://csrp.inl.gov/Documents/CSS_Defense_in_Depth_Oct09.pdf [Accessed 2010-03-10]

KoreK, (2004), *chopchop (Experimental WEP attacks),* forum post at NetStumbler. Availabe online: http://www.netstumbler.org/f50/chopchop-experimental-wep-attacks-

12489/ [Accessed 2010-03-08]

Norman, Thomas. (2007), *Integrated security systems design: concepts, specifications, and implementation.* Amsterdam: Elsevier Butterworth-Heinemann.

Olvosson, Tomas. (2006), *AppGate de-perimeterization* Available online: http://www.ossir.org/windows/supports/2006/2006-10-09/AppGate%20de-perimeterization.pdf [Accessed 10.3.09]

Panko, Raymond. (2010), *Corporate Computer and Network Security, 2nd Edition*. Upper Sadle River: Prentice Hall

Pelliccioni, Carlo, (2008), *OWASP Backend Security v1.0 BETA*. Available online: http://www.lulu.com/items/volume_64/5808000/5808965/9/print/5808965.pdf [Accessed 10.04.30]

Peterson, Dale. (2007), *New IDS Signatures for Modbus TCP,* Release notes. Available Online: http://www.digitalbond.com/index.php/2007/04/27/new-ids-signatures-for-modbus-tcp/ [Accessed 10.04.23]

Pfleeger, Charles., Pfleeger, Shari Lawrence. (2007), *Security in Computing, 4th edition*, Boston: Pearson Education.

Shinder, Thomas W, (2005), *Remote Access VPN and a Twist on the Dangers of Split Tunneling*. Available Online: http://www.isaserver.org/tutorials/2004fixipsectunnel.html [Accessed 10.04.29]

Stouffer, K., Falco, J., Scarfone K., (2008) *Guide to Industrial Control Systems (ICS) Security.* Final Public Draft, Special Publication 800-82. U.S. National Institute of Standards and Technology. Available Online: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf [Accessed 10.4.16]

Trappe, Wade. (2006), *Introduction to Cryptography with Coding Theory, Second Edition*, Upper Saddle River: Pearson Education.

Smart Card Alliance (2005), *FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems.* Available online: http://www.smartcardalliance.org/resources/lib/FIPS_201_PAC_White_Paper_FINAL_092105.pdf [Accessed 10.04.13].

Srisuresh, P.; Holdrege, M (1999) *IP Network Address Translator (NAT) Terminology and Considerations*, Request for comments 2663. Available online: http://tools.ietf.org/html/rfc2663 [Accessed: 10.05.03]

Swedish Emergency Management Agency (SEMA), (2008): *Guide to Increased Security in Process Control System for Critical Societal Functions.*

Swedish Emergency Management Agency (SEMA), (2006): *Basic level for information security (BITS)*